TABLE OF CONTENTS

INTRODUCTION

The State of Michigan's Teradata data warehouse is a centralized repository of data used to support State agencies' decision-making and business processes. The DHS Office of Child Support's (OCS) Michigan Child Support Enforcement System (MiCSES) Data Warehouse contains one subset of the data stored within the Teradata system. Department of Information Technology MiCSES (DIT-MiCSES) staff maintains and operates the MiCSES Data Warehouse on behalf of OCS. Much of the data stored on the MiCSES Data Warehouse is considered sensitive or confidential. DIT-MiCSES staff extracts data from source systems, transforms and formats the data, and loads the data into the MiCSES Data Warehouse. OCS staff and their contractual partner agencies (Friends of the Court and Prosecuting Attorneys) use analytical tools to query data stored on the MiCSES Data Warehouse to obtain accurate and timely information to support business decisions and for State and federal reporting.

OBJECTIVES AND SCOPE

The Office of Internal Audit performed an audit of the MiCSES Data Warehouse. The objectives of our audit were:

1. To assess the effectiveness of the controls over the process of granting and monitoring access to sensitive and confidential data stored in the warehouse.

2. To assess the effectiveness of MiCSES Data Warehouse efforts to ensure the integrity and accuracy of the data stored in the MiCSES Data Warehouse.

Our review primarily covered the period June 01, 2006 through February 01, 2007. The scope of the audit included reviewing appropriate records, policies, and documents we felt necessary to satisfy our objectives. We obtained background information related to

the MiCSES Data Warehouse and the organizational structure that supports the warehouse functions. We performed a risk assessment and established audit objectives. We obtained and analyzed OCS polices and procedures as they related to granting and monitoring system access and handling federal tax information. We tested security and access controls including an evaluation of the completeness and accuracy of access request forms, termination of user access accounts, and a high-level analysis of system administration accounts. We tested data integrity and accuracy controls including the completeness and accuracy of data located in key fields of some of the most frequently accessed and relied upon warehouse tables.

EXECUTIVE SUMMARY

For objective one, we concluded that Security and Access Controls could be strengthened. We noted eight (8) reportable conditions, findings 1-8.

For objective two, we concluded that Data Integrity and Accuracy Controls were generally effective. However, we noted one (1) reportable condition, finding 9.

AGENCY RESPONSE

OCS management agrees with all of the findings and recommendations. OCS management has established corrective action plans for all findings and has partially implemented corrective action for findings 1 and 2.

FINDINGS AND RECOMMENDATIONS

Security and Access Controls

User Access, Monitoring, and Tax Information Policies

1. OCS user access, monitoring, and tax information policies do not specifically address the MiCSES Data Warehouse environment.

Having policy that addresses granting and monitoring access of users with the ability to view critical and sensitive child support data and federal tax data located on the warehouse would help strengthen compliance with State and Federal regulations.

During our review we determined that critical and sensitive child support data as well as federal tax data resides on the MiCSES Data Warehouse. OCS Policy AT 2006-004 (Policy for Granting, Changing and Deleting Access to Computer Systems for IV-D Work; Accessing, Disclosing and Avoiding Conflicts of Interest in MiCSES; and Revised MiCSES Security Forms) and AT 2006-013 (Procedures for Monitoring MiCSES User Access) only briefly mention the MiCSES Data Warehouse. Policy AT 2006-005 (Internal Revenue Service (IRS) and State of Michigan Tax Return Information) does not mention the MiCSES Data Warehouse at all.

WE RECOMMEND that OCS update user access, user monitoring, and tax information polices, or create new ones, to specifically address the MiCSES Data Warehouse environment.

Security and Access Policy Enforcement

2. OCS should more strictly enforce policy AT 2006-004, AT 2006-005, and AT 2006-013 as they relate to the MiCSES Data Warehouse environment. While the noted policy AT's do not always specifically address the MiCSES Data Warehouse environment (See Finding 1), there are references to the warehouse in some of the language and most of the forms included with these AT's. In addition, it is implied that these policy AT's apply to the MiCSES Data Warehouse environment.

AT 2006-004 stipulates duties of the Authorized Requester/IV-D Contact that include, but are not limited to, the following:

A) Ensuring that the DHS 393 (MiCSES Request for Computer Access) form is properly completed and the access requested is appropriate to the employee's or contractor's job functions.

B) Ensuring that once each year every MiCSES user signs a new copy of the Michigan Department of Treasury 4062 (State of Michigan Agency Employee Confidentiality Agreement) or 3337 (Vendor, Contractor or Subcontractor Confidentiality Agreement) forms, and

C) Immediately submitting a DHS-392 (MiCSES Request to Delete Computer Access) form to the MiCSES helpdesk whenever an employee or contractor no longer needs access.

AT 2006-005 states that "each employee and any contractor that accesses federal or state tax information must sign the appropriate form (Department of Treasury form 3337 for vendors, contractors, or subcontractors or Department of Treasury form 4062 for State of Michigan staff)" to "certify that (s)he understands the policies, procedures and penalties related to safeguarding tax information before (s)he is granted access." AT 2006-013 states that "system access for MiCSES and Data Warehouse users will automatically be revoked if there has been no activity in the previous 90 days."

We tested a sample of 32 active Data Warehouse user accounts to determine if the policies appeared to be functioning appropriately.

- For 11 of the 32 active accounts sampled, the user is no longer employed (retired or separated).

Of the remaining 21 active accounts sampled we noted:

- Three of the access request forms did not specifically request access to the data warehouse
- Four users did not have current Department of Treasury Confidentiality agreements (Form 3337 or 4062) on file

Not strictly enforcing the noted Policy AT's diminishes OCS's compliance with State and Federal laws and regulations regarding unauthorized access to critical and sensitive child support and federal tax information.

WE RECOMMEND that OCS more strictly enforce policy AT 2006-004, AT 2006-005, and AT 2006-013 as they relate to the MiCSES Data Warehouse environment.

Access Request Forms

3. Access Request Forms used by MiCSES Project staff members are not the access request forms as stated in OCS Policy AT 2006-004.

OCS Policy AT 2006-004 is directed to all PA, FOC, OCS, DIT, MiCSES Project, and AG (Attorney General) staff. This AT provides the current OCS policy for granting, changing and deleting access to computer systems for IV-D work; accessing, disclosing and avoiding conflicts of interest in MiCSES; and revised MiCSES security forms. This AT requires that IV-D staff use the DHS-393 form to request access to IV-D systems, including the MiCSES Data Warehouse. In addition,

the application and scope section of this AT states that "All guidelines and regulations cited in this AT are mandatory for all organizations that have employees or contractors who access MiCSES."

Not using the request for access forms as stated in the AT promotes inconsistency and confusion among users and those processing the forms.

MiCSES Project staff use the DIT-0200 Staff Request For Computer Access form to request, change, or delete access to MiCSES and the MiCSES Data Warehouse and not the DHS 393 as stated in the AT. This form is made available to them on the OCS Inside (internal) web site.

WE RECOMMEND that OCS update Policy AT 2006-004 to include the access request form used by DIT-MiCSES staff to request, change, or delete access or require all users to use the DHS 395, DHS 393, and DHS 392 forms to request, change, or delete access as required by policy document AT 2006-004.

Authorized Requesters

4. OCS has not required all IV-D offices to submit their list of Authorized Requesters/IV-D Contacts.

Policy AT 2006-004 requires that each IV-D office designate its Authorized Requesters/IV-D Contacts and provide a list of these individuals to MiCSES Helpdesk and OCS Financial Management Division by June 30, 2006.

We obtained the most recent list of Authorized Requesters from MiCSES Helpdesk management on 9/12/06. Many IV-D offices had no Authorized Requesters/IV-D Contacts identified on the list that was provided.

Authorized Requester's responsibilities include granting and monitoring access to systems used for IV-D work as well as ensuring that appropriate case disclosure forms and Department of Treasury confidentiality agreements are on file. Not having individuals identified as Authorized Requesters/IV-D Contacts at each IV-D office increases the risk that system users are not appropriately authorized to access IV-D information systems and that OCS is not complying with Federal and State laws related to confidentiality and conflict of interest.

WE RECOMMEND that OCS ensure all IV-D offices submit their list of Authorized Requesters as required by policy AT 2006-004.

System Administration Accounts

5. Not all data warehouse administration functions had unique individual user accounts to perform their job functions.

Acceptable industry standards require that all system administration functions maintain unique individual user accounts to perform their job functions.

We noted that there were 2 user accounts (csesadmin and csespassw) that were being shared by multiple staff members to perform their job functions. These user accounts were used to perform sensitive and critical functions such as system level administration, database administration, security administration, and user account creation and modification.

Employing shared user accounts to perform sensitive and critical job functions diminishes management's ability to identify and track the activities a specific individual performs related to the system. Using unique individual user accounts would help management to hold those users that perform sensitive and critical functions accountable for their activities performed in administering the system.

WE RECOMMEND that OCS ensure all warehouse users that perform system administration, development, and help desk functions, have a unique individual user account to perform and track the activities they perform.

Timeliness of Deleting User Accounts

6. The process followed to delete user accounts from accessing the data warehouse once a request is made should be more strictly enforced to ensure it is accomplished in a timely manner.

   The National Institute of Standards and Technology (NIST) Generally Accepted Principles and Practices for Securing Information Technology Systems (publication 800-14) states "an organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users."

   During testing of data warehouse user accounts we noted that 4 of the 25 (16%) accounts in our sample population had not been deleted or deactivated within a reasonable time frame (typically 24-72 hours). These 4 accounts in which the delete

request forms were signed between 3/31/04 and 8/18/06 were still active as of 10/13/06.

Not deleting user accounts in a timely manner from the time of request could allow the user or other individuals with knowledge of the user account, to inappropriately access data warehouse data and view confidential or sensitive information that is not meant to be viewed as part of their job function.

WE RECOMMEND that OCS more strictly enforce the process followed to delete user accounts from accessing the data warehouse to ensure it is accomplished in a timely manner.

Data Share Agreements with Other Departments

7. Some of the data share agreements between OCS and other Departments/Agencies to access MiCSES Data Warehouse data appear to be outdated.

OCS provides access to data maintained on the CSES Data Warehouse to several State Departments and agencies based upon written data share agreements. We were informed that access was granted to Treasury, DCH, Judiciary, and the Unemployment Agency (DLEG) based upon written data share agreements between these Departments and DHS.

We obtained and reviewed at a high level the data share agreements in place between DHS and Treasury, DCH, and the Unemployment Agency. We were unable to locate a data share agreement in place between DCH and Judiciary. Some of the data share agreements we reviewed appeared to be outdated, which may mean that the agreement is expired or that OCS is operating without an agreement in place.

WE RECOMMEND that OCS review the data share agreements with Treasury, Unemployment Agency, DCH, and Judiciary as they pertain to the MiCSES Data Warehouse to ensure that they are still appropriate as drafted and that they are current and still applicable.

Temporary Access Privileges

8. MiCSES Data Warehouse functionality does not permit the end-dating of a user's access privileges when they request temporary access to the data warehouse.

MiCSES Request for Computer Access form (DHS 393) allows an end user to request temporary access until a specified date. We were informed during discussions with MiCSES and contractor management that there is no way to end-date a user's access to the data warehouse. It is the responsibility of the end user to send in the delete form (DHS 392) at the end of the temporary access period.

Industry standards and strong internal controls suggest that the control of deleting a user's access after a temporary access request expires should not be the responsibility of the end user but should be the responsibility of security administration staff. If an end-user forgets to send in the required delete form, their user ID will remain on the system and they may have access to data or functions that are not required or intended for long term use.

WE RECOMMEND that OCS add functionality to permit end-dating of a user's access privileges to the MiCSES Data Warehouse administrative tools. If this system change is not possible or is not cost beneficial, OCS should implement a

compensating control to ensure that a temporary user's access privileges be revoked on the requested date.

Data Integrity and Accuracy Controls

Separation of Duties

9. There is not a separation of duties between individuals that make changes to the data warehouse data and individuals that monitor what changes were made.

Strong internal controls suggest that there should be a separation of duties between job functions that have the ability to actually change data and job functions that monitor the changes to data.

Within the MiCSES Data Warehouse environment there are log files that record changes made to the data. There are administrative tools that can be accessed to detect the changes made. In the current environment only database administrators (DBA's) have the ability to change the data and only DBA's can view the log files to detect what changes were made.

Having the ability to change data within the warehouse without a third party's knowledge and oversight could allow the DBA's to inadvertently or inappropriately make changes to the data that was not authorized. Combined with the fact that system administrators have a shared User ID (Finding 3) makes it extremely difficult to detect when a specific individual has made changes to the data and what those changes were.

WE RECOMMEND that OCS ensure that a separation of duties exist between individuals that can make changes to warehouse data and individuals that monitor the log files to detect if inadvertent or inappropriate changes were made.